Reference Material for:

Agenda Item 2
SAC Policies and Directions

Slide 3
Acceptable Use Policy for IT Assets

Includes:

- Acceptable Use of Information Technology Assets Policy
- Acceptable Use of Information Technology Assets Guidelines
- Acceptable Use of King County Information Assets FAQs
- Employee and Third Party Policy for Information Technology Security and Privacy Policy
- Acknowledgement of Information Technology Security Responsibilities and Confidentiality Guidelines

King County

Office of Information
Resource Management

Information Technology Governance Policies, Standards and Guidelines

Title	Document Code No.
Acceptable Use of Information Technology Assets Policy	
Chief Information Officer Approval / Date	Effective Date.
Revision Date: 9-29-07	

1.0 PURPOSE:

This policy provides a common standard for the use of King County Information Technology Assets and advises users of these resources of acceptable and prohibited uses. King County provides its users with Information Technology Assets and resources, including workstations, Internet access and electronic communications services for the performance and fulfillment of job responsibilities. Prudent and responsible use begins with common sense and includes respect for the public's trust, the larger networked computing community and the access privileges that have been granted. The use of such resources imposes certain responsibilities and obligations on users and is subject to King County policies and applicable local, state and federal laws. Prohibited use of computing and network resources can lead to consequences affecting the individual user, many other users, and cause service disruptions.

2.0 APPLICABILITY:

King County Workforce Members who are using King County Information Technology Assets.

3.0 REFERENCES:

3.1 Enterprise Information Security Policy

3.2 King County Information Privacy Policy

3.3 Password Management Policy

3.4 Employee Code of Ethics KCC 3.04

3.5 King County Board of Ethics Advisory Opinion 96-08-1146

4.0 DEFINITIONS:

4.1 **Authorization:** The right or permission to use a computer resource.

4.2 **Authorized User:** A user with the right or permission to use a computer resource.

4.3 **Computing Resources:** Any computer based system available to a King County employee. This can be a computer, database, network device, server, printer etc.

4.4 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics:

- Not easily replaced without cost, skill, time, or other resources;
- Part of the Organization's identity, without which the Organization may be threatened.

4.5 **Minimal Personal Use**: Use that:

- Is brief in duration and frequency;
- Does not interfere with or impair the employee's ability to perform work;
- Does not interfere with or impair the conduct of official County business;
- Results in negligible or no expense to the County;
- Is not a Prohibited Use of Information Technology Assets as identified in section 5.3 in this policy.

4.6 **Organization:** Every county office, every institution, and every department, division, board and commission.

4.7 **System**: Software, hardware and interface components that work together to perform a set of business functions.

4.8 **User:** Any individual utilizing or affecting county computer resources or information technology resources including but not limited to performing work for King County utilizing a personal computer, workstation, laptop or terminal, including but not limited to any employee, contractor, consultant, or other worker.

Note: the term "user" is used in the general sense and is not intended to imply or convey to an individual any employment status, rights, privileges, or benefits.

4.9 **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

Note: the term "workforce member" is used in the general sense and is not intended to imply or convey to an individual any employment status rights, privileges, or benefits.

5.0 POLICIES:

5.1 **Ownership**: King County Information Technology Assets are the property of King County government.

5.2 **Acceptable Use of Information Technology Assets:** Users shall ensure that King County Information Technology Assets are used appropriately for King County business. Users shall use these Information Technology Assets to increase productivity, facilitate the efficient and effective performance of their duties, and meet the daily operational and business requirements of King County, including but not limited to the following illustrative list, to:

5.2.1 Perform assigned responsibilities and duties;

5.2.2 Support King County and Organization activities;

5.2.3 Access authorized work-related information;

5.2.4 Communicate and collaborate with colleagues on work-related issues;

5.2.5 Improve work-related skills when approved by management;

5.2.6 Use applications and access information available on King County's Internet and Intranet sites;

5.2.7 Access Internet hosted on-line reference and information sources such as phone directories, online dictionaries, search engines, subscription resources, or mapping and weather services if such use is appropriate for business use, adds value to the Organization, increases employee efficiency, or avoids costs that would otherwise be incurred by King County for such referenced services;

5.2.8 Access Internet based training resources approved and/or provided by King County;

5.2.9 Perform statutory and regulatory activities;

5.2.10 Comply with King County information technology security policies, standards, procedures and methods, and federal, state, and local laws concerning computers, networks and personal conduct;

5.2.11 Interact for personal use by employees with human resource, time accounting, compensation, and employee benefits and health administration programs managed by or administered for King County.

5.3 **Prohibited Use of Information Technology Assets:** Users shall refrain from using King County Information Technology Assets for prohibited uses at all times, including during breaks or outside of their regular business hours. Prohibited use of Information Technology Assets is subject to disciplinary action up to and including termination from county employment. Prohibited uses includes but is not limited to the following illustrative list of actual or attempted use of Information Technology Assets to:

5.3.1 Conduct private or personal for-profit or unauthorized not-for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;

5.3.2 Conduct any political activity;

5.3.3 Conduct any solicitation for any purpose except those officially sanctioned by King County such as the County Charitable Campaign;

5.3.4 Access any restricted, non-public Computing Resources, databases, Systems, etc. inside or outside of King County to which they may have legitimate access, to perform their assigned duties, for non-assigned (personal) purposes;

5.3.5 Conduct any unlawful activities as defined by federal, state, and local laws and/or regulations;

5.3.6 Create, access, display or transmit sexually explicit, indecent, offensive, harassing or intimidating, obscene, pornographic, defamatory, libelous material or material that could reasonably be considered discriminatory, offensive, threatening, harassing, or intimidating, except as a necessary part of bona fide work related activities;

5.3.7 Create, access, or participate in online gambling;

5.3.8 Infringe on any copyright, trademark, patent or other intellectual property rights, including copying and/or using software, images, music, movies, or other intellectual property;

5.3.9 Make copies of King County licensed software for use on non-King County computers unless explicitly authorized by the licensing agreement;

5.3.10 Knowingly perform any activity that could cause the loss, corruption of, or prevention of rightful access to data or the degradation of System or network performance;

5.3.11 Distribute King County data and information without following appropriate disclosure processes or obtaining proper authorization;

5.3.12 Engage in any activity that endangers the public;

5.3.13 Engage in any activity that results in additional cost to King County that would not normally be incurred as part of doing business;

5.3.14 Attempt to subvert the security of the King County network or network resources outside King County;

5.3.15 With the exception of authorized personnel having proper permission to do so, intercept communications of any type, intended for other persons or Systems;

5.3.16 With the exception of authorized personnel doing bonafide work and following the provisions of the Password Management Policy, use another King County user’s access privileges or user account for any reason;

5.3.17 Attempt to modify or remove computer equipment, components, software, or peripherals without proper authorization;

5.3.18 Monitor or record the electronic activities or conversations of other individuals unless explicitly authorized and in the performance of properly assigned duties;

5.3.19 Scan or monitor ports or network nodes unless explicitly authorized and in the performance of assigned duties by the organization responsible for the target Information Technology Assets;

5.3.20 Knowingly access, use, copy, modify, or delete files, data, user accounts, access rights, logs, applications, system functions, drivers, or disk space

allocations associated with King County Information Technology Assets without proper authorization;

5.3.21 Knowingly create or forward hoaxes, chain letters, Ponzi, or other pyramid schemes of any type, regardless of content, sources or destinations;

5.3.22 Forge email header information;

5.3.23 Knowingly download, install or run security programs or utilities that reveal weaknesses in the security of a System without Organization management authorization;

5.3.24 Knowingly circumvent user authentication or security of any host, network or account no matter whether it belongs to King County or some other entity;

5.3.25 Knowingly mask the identity of an account or machine without specific and properly authorized authority, including but not limited to sending anonymous email;

5.3.26 Knowingly hack into Systems and databases or act to disrupt Systems or cause unnecessary network congestion or application delays;

5.3.27 Knowingly interfere with or unreasonably deny service to any other authorized user, unless duly authorized;

5.3.28 Knowingly use any program/script/command, or send messages of any kind, with the intent to interfere with or disable a user's session via any means, locally or through the network except as identified in 5.3.27 above;

5.3.29 Knowingly establish connections that create routing patterns that are inconsistent with the effective and shared use of King County Information Technology Assets;

5.3.30 Knowingly use King County Information Technology Assets to engage in acts that deliberately waste Information Technology Assets or unfairly monopolize these resources to the exclusion of others.

5.4 **Minimal Personal Use:** Users may use King County Information Technology Assets for Minimal Personal Use, provided that the use is not prohibited as defined in section 5.3, and provided the use has the appearance of professionalism even if it is not used in a public setting.

5.5 **No Expectation of Privacy:** Although users may be expected to maintain the privacy and confidentiality of information to which they have access, they are not guaranteed personal privacy for any activity in which they engage utilizing County Computing Resources. This includes legitimate county purposes, Minimal Personal Use, violations of acceptable use or any other use. This includes, but is not limited to, word processing documents, spreadsheets, databases, electronic and voice mail, and Internet access. Users should be aware that all activity undertaken on any King County Information Technology Assets, including legitimate county purposes, Minimal Personal Use, violations of acceptable use or any other purpose, is subject to monitoring, recording and intervention by Organization management for the purpose of System update, maintenance, security and compliance with countywide and

Organization-specific policies and standards. Any use of King County Information Technology Assets constitutes user consent to such monitoring, recording and intervention. Users expecting privacy for their Minimal Personal Use should use a different means of communication. Users should be aware that electronic communications could be forwarded, intercepted, printed, and stored by others and are not subject to personal privacy expectation and may be disclosed pursuant to public disclosure laws and rules of discovery in the event of lawsuits.

5.6 **Review and Inspect:** Organizations reserve the right to retrieve and read any data composed, transmitted or received through online connections and/or stored. Electronic communications shall be open to inspection or review by Organization management to comply with local, state and federal regulations as well as any applicable policies.

5.7 **Notice of Acceptable Use:** Organizations shall provide notice of this policy to all users of King County Information Technology Assets by displaying an Acceptable Use Banner on all computers as part of the standard log-on procedure with the following language as a minimum standard:

"This system is the property of King County and is provided for authorized business use only as defined in the King County Acceptable Use of Information Technology Assets policy. Any use of this system may be monitored, recorded, audited and disclosed to authorized County and/or law enforcement personnel. Unauthorized or improper use of this system may result in discipline, up to and including termination, as well as potential civil or legal penalties. By using this system you indicate your awareness and consent to the above policy."

A similar banner must be displayed on all information technology points of entrance into King County including but not limited to virtual private networks (VPN), public wireless access points, and dial-in modem connections.

5.8 **Prior Approval to Access Unacceptable Content:** For users, who as part of their regular job responsibilities access Internet web sites generally considered to be unacceptable, Organization management must provide written approval in advance to authorize such access.

5.9 **Investigate Prohibited Use:** Organizations shall investigate violations of this policy on a case-by-case basis and discipline users according to King County policy, guidelines and practices.

6.0 RESPONSIBILITIES:

6.1 **Users** understand the expectations of this policy and accept personal responsibility for adhering to its provisions.

6.2 **Organization management** makes users aware of this policy and educates them about its content and requires that employees acknowledge receipt of such policy and the impacts of violating it.

6.3 **Organization IT management** ensures that at a minimum all PCs and Servers display the "Notice of Acceptable Use" above.

King County

Office of Information
Resource Management

Information Technology Governance Policies, Standards and Guidelines

Title	Document Code No.
Acceptable Use of Information Technology Assets Guidelines	
Chief Information Officer Approval — Date	Effective Date.
Revision Date: 9-29-07	

1.0 PURPOSE:

These guidelines advise users of King County Information Assets on acceptable and prohibited uses. King County provides its users with Information Technology Assets and resources, including workstations, Internet access and electronic communications services for the performance and fulfillment of job responsibilities. Prudent and responsible use begins with common sense and includes respect for the public's trust, the larger networked computing community and the access privileges that have been granted. The use of such resources imposes certain responsibilities and obligations on users and is subject to King County policies and applicable local, state and federal laws. Prohibited use of computing and network resources can lead to consequences affecting the individual user, many other users, and cause service disruptions.

These guidelines, while not exhaustive, are intended to provide illustrations and guidelines for best practices of acceptable conduct by users of King County Information Technology Assets.

2.0 REFERENCES:

2.1 Enterprise Information Security Policy

2.2 Acceptable Use of Information Technology Assets Policy

2.3 King County Information Privacy Policy

2.4 Password Management Policy

2.5 Employee code of Ethics KCC 3.04

2.6 King County Board of Ethics Advisory Opinion 96-08-1146

3.0 DEFINITIONS:

3.1 **Authorization:** The right or permission to use a computer resource.

3.2 **Authorized User:** A user with the right or permission to use a computer resource.

3.3 **Computing Resources:** Any computer based system available to a King County employee. This can be a computer, database, network device, server, printer etc.

3.4 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics:

- Not easily replaced without cost, skill, time, or other resources;
- Part of the Organization's identity, without which the Organization may be threatened.

3.5 **Minimal Personal Use**: Use that:

- Is brief in duration and frequency;
- Does not interfere with or impair the employee's ability to perform work;
- Does not interfere with or impair the conduct of official County business;
- Results in negligible or no expense to the County;
- Is not a Prohibited Use of Information Technology Assets as identified in section 5.3 in the Acceptable Use of Information Technology Assets Policy.

3.6 **Organization:** Every county office, every institution, and every department, division, board and commission.

3.7 **System**: Software, hardware and interface components that work together to perform a set of business functions.

3.8 **User:** Any individual utilizing or affecting county computer resources or information technology resources including but not limited to performing work for King County utilizing a personal computer, workstation, laptop or terminal, including but not limited to any employee, contractor, consultant, or other worker.

Note: the term "user" is used in the general sense and is not intended to imply or convey to an individual any employment status, rights, privileges, or benefits.

3.9 **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

Note: the term "workforce member" is used in the general sense and is not intended to imply or convey to an individual any employment status rights, privileges, or benefits.

4.0 GUIDELINES:

4.1 Daily Use

4.1.1 Users should not engage in any activity that would compromise the security and privacy of King County information technology resources, including but not limited to disabling virus protection, patch management or any other type of desktop management software.

4.1.2 Users should be mindful of the impact their activities have on King County shared Information Technology Assets and other users and on the need to be responsible stewards of the public's trust.

4.1.3 Users should not use King County Information Technology Assets for games, Internet radio or music, instant messaging or Internet chat applications.

4.1.4 Users should avoid using King County Information Technology Assets to watch streaming video unless necessary in the course of their duties.

4.1.5 Users should log off the network or have a password-protected screen saver in operation when they leave their PC unattended for more than five (5) minutes.

4.1.6 Users should log off the network at the end of the day since engaging a password protected screen saver is not recommended for overnight protections.

4.2 **Privacy**

4.2.1 Users should respect the privacy of others.

4.2.2 Users should use privacy screens in public areas where confidential information must be accessed.

4.2.3 Users should not forward information identified as “confidential” or “attorney client privileged” or “privileged” without permission of the author.

4.3 **Internet Use**

4.3.1 Users who inadvertently access unacceptable content on the Internet should notify organization management and provide an explanation of how, when and why the access happened.

4.3.2 Users should not post King County information to external newsgroups, bulletin boards, or other public forums without prior authorization.

4.3.3 Users should not make unauthorized statements or commitments on behalf of King County or the Organization, or post an unauthorized home page or similar web page.

4.4 **Electronic Communications**

4.4.1 Users should not access personal internet email accounts. Accessing personal mail bypasses several layers of security protection and can introduce malicious software into King County Systems.

4.4.2 Users should use extreme caution when opening email attachments, especially those received from unknown senders. These attachments may introduce malicious code into the King County network or Systems, such as viruses, logic bombs, or Trojan horses.

4.4.3 Users should clearly and accurately identify themselves on all electronic communications.

4.5 **Downloading Software**

4.5.1 Users should be aware that downloading of any software products using King County Information Technology Assets may be subject to licensing and contractual agreements.

4.5.2 Users should not download software of any kind from the Internet without the knowledge of their IT group. Such downloads can be accompanied by malicious code that could adversely affect King County's network or Systems.

4.5.3 Users should not use King County Internet access to download games or other entertainment software, or play games.

4.6 **Use of Information Technology Assets**

4.6.1 Users who access external networks should abide by the policies and procedures of these networks.

4.6.2 Users should exercise good judgment in their Minimal Personal Use of King County Internet access or email as defined in this policy. All Minimal Personal Use should be conducted during the employee's break times.

4.6.3 Users should use King County Information Technology Assets consistent with accepted Organization standards and in compliance with this policy.

4.6.4 Users should respect the confidentiality, availability and integrity of King County Information Technology Assets.

4.6.5 Users should not permit the use of King County owned Information Technology Assets by anyone not specifically authorized in this Policy. This includes, but is not limited to, use of laptops, PCs, and PDAs.

4.7 **Remote Access**

4.7.1 Users should not knowingly use remote control software on any internal or external host personal computers or Systems that organization management or Information Technology has not specifically authorized.

4.7.2 Users should not knowingly attach unauthorized modems to PCs, workstations or servers.

4.7.3 Users should not knowingly divulge dialup or dial-back modem phone numbers to anyone.

4.7.4 Users should not knowingly provide VPN access information to anyone without authorization.

Acceptable Use of King County Information Assets FAQs

1. Q: I have read that minimal use of information technology assets is allowed. What is a minimal use anyway?

   A: A minimal use is an infrequent or occasional use that does not impact your ability to perform your work and results in little or no cost to the county. This rule is similar to the one published by the Ethics Board for telephone use.

2. Q: May I send a personal e-mail using my King County e-mail account?

   A: Yes, you may send and receive personal e-mail on the King County e-mail system provided your use is minimal use and is not otherwise prohibited under the policy. Remember that any e-mail sent or received via the King County e-mail system may be subject to public disclosure under Washington State Law and/or disclosure due to legal action.

3. Q: May I access and use my personal e-mail account under the Acceptable Use Policy?

   A: Yes, you may access your personal e-mail account provided such access fits in the definition of minimal personal use. Remember, accessing your own e-mail over the internet may expose the county to viruses; users should exercise extreme caution when accessing personal e-mail.

   Generally such access should be done during non-work times (i.e. breaks, lunch time, etc.) and must not impact work flows.

4. Q: Minimal personal use requires that there is little or no cost to the county. What costs are associated with the use of the internet and/or the County's e-mail system?

   A: The County's resources are for business use. Here are two examples of how use incurs costs beyond what is allowed under minimal personal use:

   - **Using the Internet for personal use during your regular work time costs the county your wages, which are paid to you for public services.**
   - **Sending or receiving chain e-mails to friends and storing them on the e-mail server, especially if they contain photographs, requires the county to use its resources for your personal use. E-mails with photographs occupy large amounts of storage space on County owned equipment which should be used to store County data.**

5. Q: Does the new policy mean that I can use my county-provided cell phone for (limited) personal use? If so, what (if any) are the limits on its use?

   A: Cell phones are not generally considered Information Assets even though smart phones and Blackberries operate a form of Microsoft Windows. Therefore this policy does not directly address cell phone usage. Cell phone use would fall under the County's Employee Code of Ethics and any department-specific policy. Consult your supervisor for more information.

6. Q: Are my e-mail messages private?

   A: No, if you use county equipment do not expect a right to privacy for any of your e-mail communications. Email communications may be considered public records and could be subject to disclosure. Aside from disclosure, employees should consider that e-mail communications are subject to alteration by others and may be forwarded to unintended recipients. Avoid these potential problems by treating e-mail communications as another form of business correspondence.

7. Q: What happens if I receive a pornographic e-mail/offensive spam?

   A: First of all you should not open an e-mail from anyone that you do not know. Messages of this type often contain malicious code that can compromise the network. That said, don't panic; this happens occasionally. Mistyped internet web site addresses can result in accessing inappropriate sites and e-mail recipients have little control over the spam they receive. If you receive any kind of spam (offensive or otherwise) simply delete it. If you inadvertently access an inappropriate web site, close your browser immediately.

8. Q: Is personal use of IT resources limited to breaks and lunch? If so, does that mean that I can't call my car-pool/doctor/childcare/.... during working hours?

   A: Not necessarily. This question implies the use of the telephone which is not addressed in this policy. The ethics policy does allow minimal personal use of telephones for personal business. Consult the ethics policy and opinions for further information. The Acceptable Use Policy takes a similar position and allows you to respond to personal e-mails whether through your King County e-mail account or your personal e-mail account as long as it meets the requirements of minimal use.

9. Q: May I use my county computer to check my bank balance online?

   A: Yes, you may check your bank or deferred compensation account balances as long as such use meets the specifications of minimal use. However you cannot engage in such transactions as online banking (paying your personal bills, transferring funds, etc.) on county computers. You also may not want to engage in such activities at the office for other reasons of security. Engaging in such activities in a public or semi-public place as the office exposes you to "shoulder surfing". Shoulder surfing is the concept of others looking over your shoulder and seeing what is on your screen and sometimes watching what you type on a keyboard. In this way others, whether they are coworkers or customers may be able to see your private information and possibly even obtain your login name and password for your account.

10. Q: May I contact my union representative or shop steward over the County e-mail system?

    A: Yes, provided such use falls within the minimal rule and/or within the provisions set forth in the collective bargaining agreement covering your position or as otherwise provided by state law.

11. Q: May I use my county computer to purchase items on the internet?

    A: Employees may transact a limited amount of consumer purchasing activities on the Internet at work, as long as such use meets the specification of minimal, but may not conduct transactions for personal financial gain. For example, the purchase of a book through the Internet is acceptable, but the sale of a book is not. Buying or selling non-consumer items such as stocks or other

securities trading is prohibited by both the King County Code of Ethics and the Acceptable Use Policy as activities that can result in private financial benefit or gain.

12. Q: May I send an e-mail message to my child to make sure she arrived home safely from school?

A: Yes, such use is consistent with the policy provided the e-mail drafting is brief in duration and does not interfere with the performance of official duties. It is suggested that this may not be the most efficient method for checking on your children's welfare however.

13. Q: Are there any uses that are prohibited, even if they are brief in nature?

A: Yes, the allowance for minimal use does not apply to the following uses:

- **Conducting an outside business;**
- **Political or campaign activates;**
- **Commercial uses like advertising or selling products (including selling products on e-bay, Craig's list, etc.);**
- **Lobbying that is unrelated to official duties;**
- **Engaging in illegal or inappropriate activities;**
- **Distributing chain-e-mails. Sending bulk e-mail that is not related to official business is prohibited because it disrupts other county employees and may obligate them to make personal use of county resources.**

14. Q: There is both a policy and a guideline with the title of "Acceptable Use". What is the difference?

A: A policy is defined as a high level statement of the organizations beliefs, goals and objectives and the general means for their attainment for a specified subject area.

A guideline is a set of recommended "how-to" instructions that support some part of a policy or standard.

There is also the concept of a standard which is: A mandatory Statement of minimum requirements that support some part of a policy.

15. Q: What are the guidelines on internet use?

A: Just like the guidelines for e-mail use discussed above, any personal use of county provided Internet access must be both brief and infrequent. Extensive personal use of county provided Internet access is not permitted. In addition, your department or agency may have adopted a policy that prohibits all personal use of the Internet. Please check with your supervisor if you are unsure of your department's policies.

> **Example A: Several times over the course of a month an employee quickly uses the Internet to check her child's school website to determine if the school will end early that day. The transaction takes approximately three minutes. This use is considered minimal and permitted under the policy.**
>
> **Example B: An employee routinely uses the Internet to manage her personal investment portfolio and communicate information to her broker. This use is not permitted under the policy. The King County Code of Ethics and the Acceptable Use Policy prohibit using county resources to engage in activities that can result in private financial benefit or gain.**

Example C: An employee spends thirty to forty minutes of work time looking at various web sites related to a personal interest. This use is not permitted under the policy because it is not brief in duration and interferes with the employee's work.

16. Q: Can I watch streaming video and/or listen to internet radio through my computer at work?

    A: Yes you may, however it is not recommended unless you are doing it for work purposes such as listening to council meetings. Such activities use an excessive amount of network resources called bandwidth. This use of network bandwidth for you to listen to internet radio can result in others not being able to access their files, print documents, and access e-mail efficiently. It slows down the entire network. These activities also may be disruptive to those around you depending upon your work environment.

17. Q: My county computer can copy CDs. My computer at home cannot. Is it permitted for me to make copies of CDs using my county computer if I provide the blank CDs there is no cost to the County, right?

    A: You are correct relative to the cost of the CDs if you provide the blanks. However this would still be a violation of the policy because making copies of CDs is a time consuming process and would violate the definition of minimal use in two areas:

    - **Not brief in duration;**
    - **Would probably interfere with your ability to perform your work.**

    In addition copying of CDs even for personal use is a violation of the Digital Millennium Copyright Act of 1998.

18. Q: My county computer has a DVD player. Can I bring a DVD movie in to the office to watch on my breaks and lunch?

    A: This would be permitted under the Acceptable Use Policy as long as you kept the activity to your breaks and lunch times; however you should consider other impacts. Is this activity likely to interfere with the ability of others to do their jobs? What would be the perception of a customer or constituent observes you watching a DVD? You should consult your supervisor or manager. As a general rule if watching the DVD is for entertainment purposes and not work related it is not recommended.

19. Q: What are the Acceptable use guidelines and what happens if I fail to follow one of the guidelines?

    A: The guidelines are not part of the policy but rather are illustrations of best practices. The guidelines exist to inform county employees about how to use the public's information technology assets assigned to them responsibly and prudently. If the county experiences problems associated with continued use that is currently suggested as contrary to best practices under the guidelines, the county may seek to revise its policy to outright prohibit such use. All of us are responsible to ensure we use these assets appropriately

King County

Office of Information
Resource Management

Information Technology Governance Policies, Standards and Guidelines

Title	Document Code No.
Employee and Third Party Policy for Information Technology Security and Privacy Policy	
Chief Information Officer Approval — Date	Effective Date.

1.0 PURPOSE:

This policy establishes the information security and privacy practices related to hiring, user access to and confidentiality of King County Information Technology Assets, training, management oversight and reporting, performance reviews, discipline up to and including separation, and procurement contracts. These practices begin before employment or contract commencement, personnel guidelines and contract language that articulate expectations for information security and privacy, and continue until separation from employment or contract termination. The intent of this policy is to reduce risks to King County from errors, theft, fraud or misuse by employees and third parties.

2.0 APPLICABILITY:

King County Workforce Members (as defined in the Acceptable Use Policy) who are using King County Information Technology Assets or Resources.

3.0 REFERENCES:

3.1 Enterprise Information Security Policy.

3.2 RCW 42.17 (Washington Public Disclosure Act).

3.3 Acknowledgement of Information Technology Security Responsibilities and Confidentiality Guidelines.

3.4 Acceptable Use of Information Technology Assets Policy.

3.5 Incident Response Guidelines.

4.0 DEFINITIONS:

4.1 **Acknowledgement of Information Technology Security Responsibilities and Confidentiality (AISRC):** This is a combination of a non-disclosure document and an acknowledgement of employee responsibilities relative to Information Technology Security and privacy.

4.2 **Computer-Related Position Of Trust:** This is a position that has elevated network and/or system privileges, including but not be limited to LAN administrators, systems

engineers, network engineers, database administrators, PC support technicians, and help desk technicians.

4.3 **Elevated Network And/Or System Privileges:** Network and/or system rights and/or responsibilities that are greater than those of a standard data user. Functions performed by individuals having these privileges may include but are not limited to:

- Creating, deleting or modifying network, e-mail, or database user accounts;
- Resetting passwords on any system;
- Performing routine network (LAN/WAN), database, or PC maintenance and support;
- Having discretion and ability to grant rights to any system or information asset higher than the user's default rights.

4.4 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization and that has one or more of the following characteristics:

- Not easily replaced without cost, skill, time, or other resources;
- Part of the Organization's identity, without which the Organization may be threatened.

4.5 **Business Owner:** The entity, in this case King County, that is responsible for protecting an Information Technology Asset, maintaining accuracy and integrity of the Information Technology Asset, determining the appropriate data sensitivity or classification level for the Information Technology Asset and regularly reviewing its level for appropriateness, and ensuring that the Information Technology Asset adheres to policy.

4.6 **Information System:** Software, hardware and interface components that work together to perform a set of business functions.

4.7 **Least Privilege:** Granting a user only those access rights required to perform official job duties.

4.8 **Non-Disclosure Agreement (NDA):** A legally binding document that protects the confidentiality of ideas, designs, plans, concepts, proprietary commercial material, vital government information, or personal information. Every NDA is subject to the provisions of the Washington Public Disclosure Act (RCW 42.17).

4.9 **Organization:** Every county office, every officer, every institution, and every department, division, board and commission.

4.10 **Separation Of Duties:** The practice of purposefully dividing roles and responsibilities, so a single individual cannot subvert a process.

4.11 **Third Party:** Any person, group of persons or organization that has a business relationship with the county.

4.12 **User:** Any individual performing work for King County utilizing a personal computer, workstation, laptop or terminal, including but not limited to any employee, contractor, consultant, or other worker. Each term is used in the general sense and is not

intended to imply or convey to an individual any employment status, rights, privileges, or benefits.

4.13 **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

5.0 POLICIES:

5.1 **Employee Acknowledgement of Information Technology Security Responsibilities and Confidentiality (AISRC).**

5.1.1 **Employee AISRC:** An employee whose job function requires access to proprietary, secure or confidential information shall be required to sign a AISRC as a condition of employment. Organizations shall maintain on file the signed AISRC.

5.2 **User Access:** Organizations must have formal documented procedures in compliance with this policy for authorizing appropriate access to Information Technology Assets that includes granting different levels of access to Information Technology Assets, tracking and logging authorization of access to Information Technology Assets, and regularly reviewing and revising, as necessary, authorization of access to Information Technology Assets.

5.2.1 **Granting Access:** The Business Owner shall explicitly grant access to Information Technology Assets based on Least Privilege to an employee or Third Party and shall not allow access by default.

5.2.2 **Gaining Access:** Employees or Third Parties shall not attempt to gain access to Information Technology Assets for which they have not been given proper access authorization.

5.2.3 **Removing Access:** Organizations shall remove access to all Information Technology Assets and remove network and resource privileges at the time an employee or Third Party is separated from King County or when an employee or Third Party no longer needs to access them.

5.3 **Management Oversight:**

5.3.1 **Oversight:** Organizations shall provide oversight for employees and Third Parties who have access to proprietary, secure or confidential information, or are working in restricted areas that may include specific supervision.

5.3.2 **Contracts:** Organizations shall include the following provision in King County procurement contracts involving proprietary, secure or confidential Information Technology Assets:

"Contractor warrants and represents that each and every Contractor employee working on this contract can meet the following requirements:

- No convictions within the past ten (10) years for crimes involving computers, moral turpitude, including fraud, perjury, or dishonesty;
- No adverse employment actions within the past ten (10) years regarding dishonesty or the use or misuse of computers;
- Contractor shall, on an annual basis, confirm that it meets the requirements of this section."

5.3.3 **Vendor NDA:** Organization shall require vendors to sign a non-disclosure agreement when the work requires the vendor to have access to proprietary, secure or confidential information.

5.3.4 **Policy Compliance:** Organizations shall require vendors to adhere to countywide and Organization-specific information security and privacy policies, standards, methods and procedures.

5.4 **Incident Reporting:** Employees and Third Parties shall report to management any incident affecting information security and privacy, and all observed and suspected security weaknesses in or threats to Information Technology Assets.

5.5 **Employee Performance Reviews:** Organizations shall instruct employees regarding compliance with countywide and Organization-specific information security and privacy policies, standards, methods, practices, and procedures for all employees in a Computer-Related Position of Trust and hold them accountable for following such policies. Where applicable and appropriate, adherence to these standards should be considered in employees' performance evaluations.

5.6 **Action for Breaches of Policies and Standards:** Organizations shall utilize appropriate actions or measures for breaches of information security and privacy policies and standards consistent with county policies. Such actions may include but are not limited to termination of access rights, reassignment, and remedial training. Under appropriate circumstances disciplinary action may be appropriate and may result in action up to and including termination and/or criminal prosecution.

5.7 **Separating Employees and Third Parties:**

5.7.1 **Separation of Employees in Computer Related Positions of Trust:** Organizations shall have formal documented procedures for removing access rights of a departing employee in a Computer-Related Position Of Trust or Third Party who has had access to Information Technology Assets.

5.7.2 **Removal of Access Rights:** Organizations shall remove all access rights to Information Technology Assets granted to the employee or Third Party who is being non-voluntarily separated.

5.7.3 **Confidential, Proprietary and Non-Public Information:** The separated employee or Third Party shall not retain, give away, or remove from county premises any county proprietary information (electronic or hardcopy) except (1) personal copies of information disseminated to the public, and (2) personal copies of correspondence directly related to the terms and conditions of employment. At the time of departure, the separated employee or Third Party shall relinquish all other county proprietary information or Information

Technology Assets in his/her custody to his/her immediate King County supervisor or designate.

5.7.4 **County Property:** At the time of separation, the employee or Third Party shall return to his/her immediate King County supervisor or designee all county property in his/her possession, including but not limited to portable computers, printers, modems, software, personal digital assistants, documentation, building keys, lock combinations, encryption keys, and magnetic access cards.

5.7.5 **Physical Access:** Organizations shall deactivate or change all physical security access codes, such as a keypad lock PIN, used to protect Information Technology Assets that are known by the separating employee or Third Party.

5.8 **Separation Of Duties:** Organizations shall structure job functions to ensure a Separation Of Duties and an audit trail of actions taken where collusion could harm King County's information security and/or privacy.

5.9 **New Employees:** Organizations shall inform new employees who access County Information Technology Assets of the countywide and Organization-specific information security and privacy policies, standards, guidelines, methods, practices and procedures.

5.10 **Existing Employees:** Organizations should provide regular updates to employees who access Information Technology Assets, including but not limited to information security and privacy awareness training, updates to Countywide and Organization-specific information security and privacy policies, standards, guidelines, methods, practices and procedures, and process for reporting information security and privacy incidents and vulnerabilities.

6.0 EXCEPTIONS:

6.1 Any agency needing an exception to this policy must follow the Information Technology Policy and Standards Exception Request Process using the Policy and Standards Request form. This form can be found on the Office of Information Resource Management policies and procedures Web page at http://kcweb.metrokc.gov/oirm/policies.aspx.

7.0 RESPONSIBILITIES:

7.1 **Organization staff** protects the integrity, availability and confidentiality of King County's Information Technology Assets by complying with countywide and Organization-specific information security and privacy policies, standards, method and procedures and the non-disclosure agreement.

7.2 **Third Party** protects the integrity, availability and confidentiality of King County's Information Technology Assets by complying with information security and privacy policies, standards, method and procedures and the non-disclosure agreement with King County.

7.3 **Organization IT management** ensures that access rights are granted and removed accurately and timely.

7.4 **Business Owner** provides clear direction to management and the appropriate IT organization on assignment of access rights to the Information Technology Assets for which they have responsibility.

7.5 **Organization management** ensures that:

7.5.1 Responses are appropriate as outlined in the Incident Response Guidelines (draft) to incident reports as described in section 5.4 or as outlined in agency specific policy or procedure.

7.5.2 Procedures are in place and are followed by staff to notify the appropriate IT organizations of creations, deletions and changes to user access rights and accounts.

7.5.3 Signed AISRCs are maintained on file.

7.5.4 All employees:

7.5.4.1 Receive appropriate Information Security and Privacy information;

7.5.4.2 Understand the countywide and Organization-specific policies, standards, methods and procedures, as appropriate; they must comply with and receive feedback on compliance during performance reviews;

7.5.4.3 Understand the terms and conditions of employment, contract or agreement, and job functions.

7.5.5 All Third Parties with access to county Information Technology Assets shall:

7.5.5.1 Receive necessary security and privacy information related to King County policies, standards, methods and procedures to ensure satisfactory levels of Confidentiality, Integrity and Availability;

7.5.5.2 Understand and comply with King County policies, standards, methods and procedures;

7.5.5.3 Understand the terms and conditions of the contract or agreement;

7.5.5.4 Have signed a King County nondisclosure agreement and maintain a copy as part of the contract;

7.5.5.5 Ensure that contracts are evaluated to contain the proper warranties regarding contractor staff;

7.5.5.6 Ensure that contractors maintain compliance with countywide and Organization-specific policies, standards, guidelines, methods, practices and procedures.

7.6 **County information security officer** provides countywide guidance and oversight on addressing information security concerns in the hiring and contracting process, in position descriptions, through training and employee reviews, and in managing access rights to Information Technology Assets.

7.7 **County information privacy officer** provides countywide guidance on addressing information privacy concerns through the use of nondisclosure agreements and in training.

King County

Office of Information
Resource Management

Information Technology Governance Policies, Standards and Guidelines

Title	Document Code No.
Acknowledgement of Information Technology Security Responsibilities and Confidentiality Guidelines	
Chief Information Officer Approval / Date	Effective Date.

1.0 PURPOSE:

This guideline provides King County Organizations information relative to when an agreement should be signed by persons in a Computer-Related Position of Trust who have access to proprietary, secure or confidential information. Included in these guidelines is a model agreement that acknowledges the individual's responsibility.

2.0 REFERENCES:

2.1 Employee and Third Party Policy for Information Technology Security and Privacy.

3.0 DEFINITIONS:

3.1 **Acknowledgement of Information Security Responsibilities and Confidentiality:** This is a combination of a non-disclosure agreement and a general acknowledgement of responsibilities relative to Information Security and privacy.

3.2 **Computer-Related Position Of Trust:** This is a position with elevated network and/or system privileges, including but not limited to LAN administrators, systems engineers, network engineers, database administrators, PC support technicians, and help desk technicians.

3.3 **Elevated Network And/Or System Privileges:** Network and/or system rights and/or responsibilities that are greater than those of a standard data user. Functions performed by individuals having these privileges may include but are not limited to:

- Creating, deleting or modifying network, e-mail, or database user accounts;
- Resetting passwords on any system;
- Performing routine network (LAN/WAN), database, or PC maintenance and support;
- Having discretion and ability to grant rights to any system or information asset higher than the user's default rights.

3.4 **Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics:

- Not easily replaced without cost, skill, time, or other resources;
- Part of the Organization's identity, without which the Organization may be threatened.

3.5 **Information Owner:** The person who is responsible for protecting an Information Asset, maintaining accuracy and integrity of the Information Asset, determining the appropriate data sensitivity or classification level for the Information Asset and regularly reviewing its level for appropriateness, and ensuring that the Information Asset adheres to policy. The information owner is one or both of the following:

- The creator of the information or the manager of the creator of the information;
- The receiver of external information or the manager of the receiver of the external information.

3.6 **Organization:** Every county office, every officer, every institution, and every department, division, board and commission.

3.7 **Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

4.0 GUIDELINES:

4.1 Organizations should have each person in a Computer-Related Position of Trust sign an Acknowledgement of Information Security Responsibilities and Confidentiality, including third parties as appropriate to their contract or agreement with King County.

4.2 The Acknowledgement of Information Security Responsibilities and Confidentiality should be signed by both the person in a Computer-Related Position of Trust and acknowledged by the supervisor or manager for this position. This should be signed prior to the person's first day working in a Computer-Related Position of Trust and annually thereafter.

4.3 Organizations shall request that other workforce members with access to proprietary, secure or confidential King County information sign the Acknowledgement of Information Security Responsibilities and Confidentiality.

4.4 After the Acknowledgement of Information Security Responsibilities and Confidentiality is signed a copy should be given to the employee, contractor, consultant, etc. and the original filed in either the departmental personnel file (in the case of employees) or maintained with the official contract file (in the case of contractors, consultants, etc.).

5.0 APPENDICES:

5.1 Model: Acknowledgement of Information Security Responsibilities and Confidentiality (see next page).